

**Monday, 17 November 2008**

**Version 1.1**

*Prepared by*

**Revision and Signoff Sheet**

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Version** | **Change reference** |
| 11/17/08 |  | 1.1 | Added Windows client exclusions.  Replaced SMS exclusions Configuration Manager exclusions. |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Version approved** | **Position** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1 Introduction 1](#_Toc214718450)

[1.1 Why Exclude 1](#_Toc214718451)

[1.2 Document Purpose 1](#_Toc214718452)

[1.3 Disclaimer 1](#_Toc214718453)

[1.4 Document Scope 2](#_Toc214718454)

[2 Exclusion Guidelines 1](#_Toc214718455)

[3 Appendix A – Best Practices for Determining Files to Exclude from Scanning 8](#_Toc214718456)

[3.1 Types of Files 8](#_Toc214718457)

1. Introduction
   1. Why Exclude

It is important to achieve a balance between ensuring a secure and virus free server environment while also not interfering with reliability and performance of each server.

A lack of exclusions with regards to virus scanning has traditionally been one of the main causes of outages with regards to applications and services. In addition, virus scanning is often a cause of performance issues.

* 1. Document Purpose

The purpose of this document is to provide guidelines for anti-virus configuration parameters, depending on the software installed on a server. These guidelines are based on Microsoft Knowledge Base, Microsoft Premier Support as well as collective field experience from Microsoft Services.

Theses guidelines apply to both memory resident ‘Realtime’ scanning as well as on-demand ‘Local Scanning’.

* 1. Disclaimer

Implementing the exclusion guidelines described in this document may make your computer or your network more vulnerable to attack by malicious users or by malicious software such as viruses. Before making these changes, it is recommended that the risks that are associated with implementing this workaround be evaluated. It is noted that in some cases, additional settings may be required in addition to those contained in the document to prevent reliability and/or performance issues.

It is at the discretion of the reader with regards to interpretation and implementation of the guidelines contained in this document.

* 1. Document Scope

This document covers anti-virus scanner settings for the following Microsoft Technologies running on Windows Client applications and Windows Server applications (and services):

1. Windows Client
   1. WSUS client
   2. Configuration Manager 2007 Clients
   3. Offline Folders
   4. Print Spooler
   5. Softgrid Client
   6. Windows Search
2. Microsoft Applications
   1. ADAM
   2. BizTalk 2004
   3. Exchange Server 2003
   4. Hyper-V
   5. Live Communications Server (LCS) 2005
   6. Microsoft Baseline Security Analyzer (MBSA) 2.x
   7. Microsoft Identity Integration Server (MIIS) 2003
   8. Microsoft Operations Manager (MOM) 2005
   9. SharePoint Portal Server (SPS) 200x
   10. SQL Server 2005
   11. Systems Center Configuration Manager 2007
   12. Systems Center Configuration Manager Clients
   13. Virtual Server (VS) 2005 (Host)
   14. Virtual PC (VPC) 2007 (Host)
   15. Visual SourceSafe 4 / 5 / 6
   16. Windows Rights Management Services (RMS)
   17. Windows SharePoint Services (WSS)
   18. Windows System Resource Manager (WSRM)
   19. Windows Server Update Services (WSUS)
3. Core Windows Server 2003 Services
   1. Active Directory
   2. ASP.NET applications
   3. Cluster Service
   4. DHCP Service
   5. File Replication Service (FRS)
   6. Internet Information Services (IIS) 5 / 6
   7. Index Service
   8. MSMQ
   9. Pagefile
   10. Print Service
   11. SMTP Service
   12. Terminal Server Licensing Service
   13. WINS Service

This document does not cover scanning of data within applications themselves. For example, it is possible to scan data within Exchange and SharePoint databases.

1. Exclusion Guidelines

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service / Application** | **Process** | **File, Extension or TCP/IP port** | **Default Folder** | **Comments** |
| ***Windows Client*** |  |  |  |  |
| WSUS client | - | wsusscan.cab  wsusscan2.cab | - | [Multiple symptoms occur if an antivirus scan occurs while the Wsusscan.cab file or the Wsusscn2.cab file is copied](http://support.microsoft.com/?kbid=900638) |
| Configuration Manager 2007 Client | - | \*.\* /s | C:\Windows\system32\CCM\Cache | Package cache folder |
| Offline Folders |  |  | c:\windows\CSC |  |
| Print Spooler | spoolsv.exe | \*.spl  \*.shd | C:\WIndows\system32\spool\PRINTERS | Print Spool service |
| Softgrid Client |  | \*.\* /s | C:\Users\Public\Documents\SoftGrid Client[[1]](#footnote-2) | Potentially also exclude sequencer files. The sequencer uses the %TEMP% and its own Scratch directory for temporary files. Example: C:\Users\<user>\AppData\Local\Temp |
| Windows Search | Searchfilterhost.exe  Searchindexer.exe  Searchprotocolhost.exe |  |  |  |
| ***Windows Server Applications*** |  |  |  |  |
| BizTalk 2004  (dependant on SQL Server, ASP.NET, . may be dependant on MSMQ)  <http://support.microsoft.com/?id=318941> | - | As required | Exclude any BizTalk file receive queue folders  IIS virtual directories used by BizTalk server (MessagingManager, BizTalkServerRepository)  Exclude any file extensions used, i.e. if you are consuming xml messages exclude scanning of .xml files. | BizTalk File Receive |
|  | - | \*.config  Global.asax | - | .config files containing application execution options. |
| Exchange Server 200x  (dependent on SMTP, IIS) | mad.exe  store.exe | \*.edb  \*.stm | *%ProgramFiles%*\Exchsrvr\MDBDATA | Exchange databases |
| <http://support.microsoft.com/?id=245822>  <http://support.microsoft.com/?id=823166>  <http://support.microsoft.com/?id=328841> |  | \*.chk  \*.log  \*.dat | *%ProgramFiles%*\Exchsrvr\MDBDATA | Exchange database logs |
|  |  | \*.\* /s | M: | Installable File System (IFS) drive (drive M). This applies to an Exchange 2000 server and only if M: drive is enabled. |
|  |  | \*.stf | *%ProgramFiles%*\Exchsrvr\MDBDATA  (or wherever database log files are stored) | Temporary files are used during the content conversion process. These files are only specific to Exchange 2000 Server. |
|  |  | \*.\* | *%ProgramFiles%*\Exchsrvr\Mtadata | Exchange MTA files |
|  |  | \*.log | C:\Exchsrvr\*%servername%*.log  (where *%servername%* is the name of the server running Exchange Server) | Exchange message tracking log files (if enabled) |
|  |  | \*.\* /s | *%ProgramFiles%*\Exchsrvr\Mailroot | Virtual server folders |
|  |  | \*.\* | %ProgramFiles%\Exchsrvr\Srsdata | Site Replication Service (SRS) |
|  |  | \*.\* | Any folders used when running offline maintenance utilities such as Eseutil.exe. |  |
| Live Communications Server (LCS) 2005  (may be dependant on SQL server or MSDE) | - | \*.mdf | C:\LC Archiving Data | Archive databases |
|  |  | \*.ldf | C:\LC Archiving Log | Archive logs |
|  |  | \*.mdf | C:\LC Data | User and Configuration databases |
|  |  | \*.ldf | C:\LC Log | User and Configuration logs |
| Hyper-V host | Vmms.exe  Vmswp.exe  Vmwp.exe | \*.vhd  \*.vsv  \*.vud  \*.vfd  \*.iso  \*.xml  \*.avhd  \*.bin | Exclude these extensions for all Hype-V related folders containing these files. | Excludes virtual machines, floppies, save states, snapshots, ISOs and configuration xml files. |
| Microsoft Baseline Security Analyzer (MBSA) 2.x  <http://support.microsoft.com/?id=900638> | - | wsusscan.cab | C:\Documents and Settings\*%username%*\Local Settings\Application Data\Microsoft\MBSA\2.0\Cache | Because the Wsusscan.cab file contains several nested cabinet files, excluding the Wsusscan.cab file itself is not typically sufficient to combat the high CPU use unless you can also specify to exclude its contents. |
| Microsoft Identity Integration Server (MIIS) 2003 | - | MicrosoftIdentityIntegrationServer.mdf  MicrosoftIdentityIntegrationServer\_log.LDF | *%ProgramFiles%*\Microsoft Identity Integration Server\data | MIIS database and log |
| Microsoft Operations Manager (MOM) 2005  (MOM Management server dependent on SQL Server. MOM Reporting dependant on IIS and SQL Server Reporting Services, MOM Web Console dependent on IIS) | - | MOMHost.exe.config | *%ProgramFiles%*\Microsoft Operations Manager 2005 | .config file contains application configuration options. |
|  |  | web.config | *%ProgramFiles%*\Microsoft Operations Manager 2005\WebConsole | Web Console .config file contains application configuration options. |
| SharePoint Portal Server (SPS) 200x  <http://support.microsoft.com/?id=320111> | - | \*.\* | *%ProgramFiles%*\SharePoint Portal Server |  |
|  |  | \*.\* | *%ProgramFiles%*\Common Files\Microsoft Shared\Web Storage System |  |
|  |  | \*.\* | *%SystemRoot%*\Temp\FrontPageTempDir | File cache for uploading user files to the document library. |
|  | owstimer.exe | Port 25 | N/A | Alerts relating to Adding, Modifying, and Deleting information from the Site.  SharePoint Portal server sends out alerts to an SMTP service on port 25. Some anti-virus applications have an option to "Prevent mass mailing worms from sending mail" in port 25. Ensure that the OWSTIMER.EXE is added to the exception list to allow it to communicate with SMTP. |
| SQL Server 2005  <http://support.microsoft.com/?id=309422> | mssql.exe  sqlagent.exe | \*.mdf  \*.ldf  \*.ndf |  | SQL database and logs |
| Microsoft Configuration Manager site servers  <http://technet.microsoft.com/en-us/library/bb932206.aspx> | - | install.map | *%ProgramFiles%*\Microsoft Configuration Manager | Prevents contention for install.map data file. |
|  |  | \*.\* | *%ProgramFiles%*\Microsoft Configuration Manager\Inboxes  (exclude file types or all files for all sub folders under this folder). | Site Server inboxes (only applies to servers providing Site Server services) |
|  |  | \*.log | *%ProgramFiles%*\Microsoft Configuration Manager\Logs  H:\Program Files\SMS\_CCM\Logs | SMS Logs |
|  |  | \*.\* | *%Drive%*\SMSPKG folder (this is typically the drive that contains the most available disk space)  (exclude file types or all files for all sub folders under this folder). | Distribution manager stores compressed copy of package. |
|  |  | \*.msg  \*.que  \*.xml | *%ProgramFiles%*\SMS\_CCM\ServiceData | Management Point (MP) (only applies to SMS 2003 Management Points) |
| Virtual Server 2005 Host  (dependent on IIS)  <http://support.microsoft.com/?id=840193> | vssrvc.exe  vmh.exe | \*.vhd  \*.vmc  \*.vsv  \*.vud  \*.vfd | Exclude these extensions for all folders on the server. | Virtual machines, floppies and save state. |
|  | - | \*.iso | Exclude this extension for all folders on the server. | ISO Image files |
| Virtual PC 2007 Host  <http://support.microsoft.com/?id=840193> | virtualpc.exe | \*.vhd  \*.vmc  \*.vsv  \*.vud  \*.vfd  \*.iso | Exclude these extensions for all folders on the server. | Virtual machines, floppies and save state.  [Virtual machines run very slowly in Virtual PC 2004 or in Virtual Server 2005](http://support.microsoft.com/?id=840193) |
| Visual SourceSafe 4 / 5 / 6  <http://support.microsoft.com/?id=274051> | - | - | Disable **any** realtime scanning on the server.  Manually scan SourceSafe server periodically. |  |
| Windows Rights Management Services (RMS) | - | \*.config  Global.asax | - | .config files containing application execution options. |
| Windows SharePoint Services (dependent on SQL Server or MSDE) | owstimer.exe | Port 25 | N/A | Alerts relating to Adding, Modifying, and Deleting information from the Site.  SharePoint Portal server sends out alerts to an SMTP service on port 25. Some anti-virus applications have an option to "Prevent mass mailing worms from sending mail" in port 25. Ensure that the OWSTIMER.EXE is added to the exception list to allow it to communicate with SMTP. |
|  | - | \*.\* /s | *%SystemRoot%*\Temp\FrontPageTempDir | File cache for uploading user files to the document library. |
| WSRM | - | Wsrm.edb | *%SystemRoot%*\system32\Windows System Resource Manager\JetDB | Accounting Database |
| WSUS  (dependent on SQL Server or MSDE) | - | \*.mdf  \*.ldf | C:\WSUS\MSSQL$WSUS\Data | WSUS MSDE database and logs (present if MSDE is used for WSUS database) |
| ***Windows Server 2003 Services*** |  |  |  |  |
| .NET Framework | - | \*.\* /s | *%SystemRoot%*\Microsoft.NET\Framework |  |
| Active Directory  <http://support.microsoft.com/?id=822158> | lsass.exe | ntds.dit  ntds.pat | *%SystemRoot%*\ntds | NTDS Database |
| <http://support.microsoft.com/?id=284947>  <http://support.microsoft.com/?id=815263> |  | edb\*.log  ntds.pat  res1.log  res2.log | *%SystemRoot%*\ntds | NTDS Logs |
|  |  | temp.edb  edb.chk | *%SystemRoot%*\ntds | NTDS Working folder |
|  |  | \*.\* /s | *%SystemRoot%*\Sysvol\sysvol | SYSVOL – This exclusion may not be necessary, please refer to TechNet article <http://support.microsoft.com/?id=815263> for details) |
|  |  | \*.\* /s | *%SystemRoot%*\Sysvol\staging areas | SYSVOL – This exclusion may not be necessary, please refer to TechNet article <http://support.microsoft.com/?id=815263> for details) |
|  |  | \*.\* /s | *%SystemRoot%*\Sysvol\staging | SYSVOL – This exclusion may not be necessary, please refer to TechNet article <http://support.microsoft.com/?id=815263> for details) |
| ASP.NET applications  (.NET Framework)  <http://support.microsoft.com/?id=312592>  <http://support.microsoft.com/?id=829978>  <http://support.microsoft.com/?id=821438>  <http://support.microsoft.com/?id=871042> | - | \*.config  Global.asax | Location will depend on where the application has been installed to. | .config file contains application configuration options.  Exclude these file types for all servers running ASP.NET applications.  Note that this issue is resolved for both Microsoft .NET Framework 1.0 and 1.1 with a hotfix (and possibly now a service pack). Please refer to <http://support.microsoft.com/?id=821438> and <http://support.microsoft.com/?id=871042> for details. |
| Certificate Server | - | Domain.edb  tmp.edb  edb.chk  res1.log  res2.log | *%SystemRoot%*\system32\CatRoot2 | Certificate Jet database and logs |
| Cluster Service  <http://support.microsoft.com/?id=321531>  <http://support.microsoft.com/?id=250355> | - | \*.\* | *%SystemRoot%*\Cluster |  |
|  |  | \*.\* /s | *%QuorumDrive%*\MSCS  (where *%QuorumDrive%* is the shared Quorum disk resource) | Cluster Quorum disk |
| DFS | - |  | The same resources that are excluded for a SYSVOL replica set must also be excluded when FRS is used to replicate shares that are mapped to the DFS root and link targets on Windows 2000 or Windows Server 2003-based member computers or domain controllers. |  |
| DHCP Service | - | tmp.edb  dhcp.mdb  dhcp.pat  j\*.log  res1.log  res2.log | *%SystemRoot%*\system32\dhcp | DHCP Jet database and logs |
| Print Service | spoolsv.exe | \*.spl  \*.shd | *%SystemRoot%*\system32\spool\PRINTERS | Print Spool service |
| File Replication Service (FRS) | - | ntfrs.jdb | *%SystemRoot%*\ntfrs\jet | <http://support.microsoft.com/default.aspx?scid=kb;en-us;815263>  File Replication Service (FRS) database – Needed for SYSVOL |
|  |  | \*.log | *%SystemRoot%*\ntfrs\jet\log | FRS logs – Needed for SYSVOL |
|  |  | edb.chk | *%SystemRoot%*\ntfrs\jet\sys | File Replication Service (FRS) working folder – Needed for SYSVOL |
| Internet Information Services (IIS) 5 / 6  <http://support.microsoft.com/?id=817442> | inetinfo.exe | \*.config  Global.asax | Location will depend on where the application has been installed to. | .config files containing application execution options.  Exclude these file types for all servers running IIS. |
|  |  | metabase.bin | *%SystemRoot%*\system32\inetsrv | IIS 5 metabase |
|  |  | MetaBase.xml  MBSchema.xml | *%SystemRoot%*\system32\inetsrv | IIS 6 metabase |
|  |  | \*.\* | *%SystemRoot%*\IIS Temporary Compressed Files | IIS temporary compressed files |
| Index Service  <http://support.microsoft.com/?id=247093>  <http://support.microsoft.com/?id=209304> | cisvc.exe  cidaemon.exe | catalog.wci | C:\System Volume Information  (in addition, exclude the catalog.wci in any other folders that contain an Index Catalog) | System catalog. |
| MSMQ | - | \*.\* /s | *%SystemRoot%*\system32\MSMQ  *%SystemRoot%*\system32\MSMQ\storage | MSMQ Queues |
| Pagefile  (present on all Windows servers) | - | Pagefile.sys | C:\ | Windows Pagefile |
| SMTP Service | - | \*.\* /s | C:\Inetpub\mailroot | Default SMTP virtual Server |
| Terminal Server Licensing Service | lserver.exe | \*.edb  \*.log  \*.tmp  \*.chk | *%SystemRoot%*\System32\LServer | License server database and logs |
| WINS Service | - | wins.mdb  winstmp.mdb  j50.chk  j50.log  res1.log  res2.log | *%SystemRoot%*\system32\wins | WINS Jet database and logs |

**Notes**

1. Any paths shown in this document are default installation paths only. Actual paths may vary (and may even be split across multiple drives as is often the case with SQL, Exchange and SMS).
2. %SystemRoot% is ‘C:\Windows’ by default and %ProgramFiles% is ‘C:\Program Files’ by default.
3. If the server was upgraded from Windows NT4.0 then the Windows folder will likely be C:\WINNT.
4. \*.\* designates that all files in the folder specified should be excluded.
5. \*.\* /s designates that all files in the folder specified and all sub-folders should be excluded.
6. Specific recommendations from antivirus software vendors may supersede the guidelines contained in this document.
7. Some of the guidelines may not be applicable with any future service packs, hotfixes or versions of any of the operating systems or applications listed in this document.
8. The TechNet articles referenced generally contain a more detailed explanation with regards to potential issues and resolutions with regards to virus scanning software. It is strongly recommended that these articles be reviewed when planning an anti-virus strategy.
9. Appendix A – Best Practices for Determining Files to Exclude from Scanning
   1. Types of Files

The exclusion guidelines contained in Section 2 of this document are product specific. For other applications (not listed above), it is often necessary to determine exclusions on a case-by-case basis. The section below provides some guidance in this area.

Files should typically be excluded based on the following criteria:

* *Locked Files -* The files are permanently locked open by a legitimate server process. Examples of these are databases such as DHCP and SQL Server, as well as files such as the Windows Pagefile.
* *Large Files -* The files are manipulated often by a legitimate server process and are typically large in size. Examples of these are copying CD/DVD images (.iso) and Virtual Machine Files (.vhd). In addition operations may also include the likes of offline maintenance on Virtual Machine Files and Exchange Server databases.
* *Temporary Files -* A large number of temporary files are written to disk by a legitimate server process. Examples of are the Spool folder and Exchange Server MTA queues.

1. Potentially also exclude sequencer files. The sequencer uses the %TEMP% and its own Scratch directory for temporary files. Example: C:\Users\<user>\AppData\Local\Temp [↑](#footnote-ref-2)